Identity Theft: What CPAs Need to Know

by Frimette Kass-Shraibman, CPA, MA, NCCPAP National Director;

Kevin Kelly, CPA, Esq.

Identity theft has become a major security issue. Between 2001 and 2003, identity theft reports tripled in the United States and reports tripled in the United Kingdom from 2002 to 2003. Identity theft is being used to launder money, fund terrorism, and for just plain old theft. A Federal Trade Commission report dated September 2003 states that 27.3 million Americans have been victims of ID theft. In the year prior to the report, ID theft cost businesses $48 billion and consumers and additional $5 billion.

Identity theft often includes Social Security Numbers (SSNs). Lawrence Maxwell, Assistant Chief Inspector, U.S. Postal Service defined identity theft as "when a thief steals key pieces of someone's identifying information, such as name, date of birth, and Social Security number, and uses the information to fraudulently apply for credit or to take over a victim's credit or bank accounts."

Misusing a SSN to receive anything of value aggregating $1,000 or more is a felony under Federal Law. The Federal Law makes it a crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal Law, or that constituted a felony under an applicable stated or local law."

How can you protect yourself and clients from being becoming victims? How can we retard growth of this crime?

SSNs and Employees

When hiring a new employee, and employer can verify the validity of the applicant's SSN by contacting the Social Security Administration (SSA). Which will verify up to five SSNs by phone (1-800-772-6270) between 7 a.m. and 7 p.m. Eastern time. Additional SSNs may be verified electronically; more additional information is available at the website **http:// www.socialsecurity.gov/employer/ssnv.htm**. SSA hopes to have an online verification system ready in 2005. Verifying an applicant's SSN is not required, but it's a good idea—especially if anything about the application or individual's credentials does not appear consistent or true.

Employers should also do background checks on employees. There are many on-line detective services that will do this for a nominal fee. This is especially important if the applicant will be handling sensitive information such as employee records or customer/client records that include birth dates and SSNs. If the employer has special confidentiality rules the integrity of an employee with access to sensitive data is critical. Employers with special confidentiality rules might include employers in such industries as financial institutions, medical/healthcare providers, accountants and attorneys. If an

employee breaches confidentiality the employer may be held liable for ensuing damages. Be sure you know whom you're hiring!

Customers and Vendors

Businesses should also verify with whom they are doing business. The proliferation of on-line credit applications, e-commerce in general, and availability of technology to create false documents has helped fuel the identity theft fires. Ask for identification form first time customers and vendors. If something doesn't look right, refusing the sale may save you money in the long run. Several banks have been sued by ID theft victims for allowing fraudsters to misuse SSNs at the bank.

However, you shouldn't ask for a customer's SSNs unnecessarily, because if you have the number and don't protect it you may be held liable for its misuse. In order to reduce to possibility of identity theft, the American Medical Association advises its members not to use SSNs to identify insured's, patients, or physicians. Many medical/healthcare providers, however, continue to ask for SSNs. There have been instances of patients using made-up numbers in order to comply with a doctor's request while protecting their information. It has been a long-time practice of health insurance providers to use SSNs instead of a policy number. This trend, however, is changing. Many health insurance companies will now use policy numbers other than the insured's SSN. If your health insurance card has your SS number on it, call the insurance company and ask them to change it.

What Individuals Should Do to Protect Themselves

To protect themselves from ID theft, individuals should not use their SSN unnecessarily. If asked for you number ask why it's needed, is it required by law to be given, who will have access to it, and how will it be protected. Unless required by law you don't have to give your SSN. However, the business may refuse to do business with you.

It's not advisable to keep your driver's license and Social Security card in the same wallet. If it's stolen, the thief has the SSN and birth date. Even family members can't be trusted with your SSN. Lesley Stahl reported that up to 9% of ID theft culprits are family members.

If you believe that you might be the conduit for ID theft or the victim, here's what you should do. First, notify your local police. Also notify the Federal Trade Commission. You can do it at www.consumer.gov/idtheft/, their online reporting site. The Social Security Administration can be notified at 1-800-269-0271 (10 a.m. to 4 p.m. Eastern time). Call and write to the three credit reporting agencies:

- Transunion at **www.transunion.com**
- Equifax at **www.equifax.com**
- Experian at **www.experian.com**

They'll flag the account if there's a credible report of ID theft.

Under the Fair Credit Reporting Act (FCRA) an individual who believes that s/he is a victim of identity theft is entitled to get from a business the records that related to the

fraud. Businesses are required to respond to such requests within 30 days. Businesses must also forward copies of the relevant records to any law enforcement agency designated by the victim. Information on the FRCA is at **www.ftc.gov**.

For more information on protecting yourself and your clients from identity theft visit these websites:

- **www.idtheftcenter.com** (Identity Theft Resource Center)
- **www.privacyrights.org** (Privacy Rights Clearing House)
- **www.usdoj.gov/criminal/fraud/idtheft.html** (United Stated Department of Justice)

Conclusion

This is a serious issue. In a recent case in the United States Attorney's Maryland office, 31 persons are being prosecuted for allegedly laundering drug money by buying life insurance policies in 17 ID theft victims. As of the date of the report, the e U.S. Attorney wouldn't confirm if the victims were alive or deceased. The possible implications are scary.

To view this article with a full bibliography, contact the NCCAPP National Office.